Université de Toulon
U.F.R. de Sciences
Mathématiques

Année 2014-15
10 février 2015

Licence de Mathématiques - L3
Modélisation - Interro

1h30

2 305 843 009 213 693 951

Exercice 1. Pour tout entier $m > 0$, on note $\pi(m)$ le nombre de nombres premiers p tels que $p \leq m$.

1. Déterminer $\pi(1)$, $\pi(2)$, $\pi(3)$, $\pi(4)$, $\pi(20)$.

2. On rappelle le théorème de Wilson :
p est premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.

Pour tout entier $j \geq 1$, on définit

$$F(j) = \left[\cos^2\Big(\frac{(j-1)!+1}{j}\pi\Big)\right]$$

où $[x]$ désigne la partie entière du réel x.

Montrer que, pour tout $j > 1$, on a $F(j) = 1$ si j est premier, et $F(j) = 0$ sinon.

3. En déduire que

$$\pi(m) = -1 + \sum_{j=1}^{m} F(j).$$

Exercice 2. Soit p un nombre premier impair.

1. Soit a un entier relatif. Rappeler la définition du symbole de Legendre $\left(\frac{a}{p}\right)$.

2. Rappeler le critère d'Euler concernant le symbole de Legendre.

3. Rappeler que vaut $\left(\frac{2}{p}\right)$ en fonction de la congruence de p modulo 8.

4. Considérons les nombres de Mersenne $M_q = 2^q - 1$ où q est un nombre premier impair tel que $p = 2q + 1$ soit premier.

Montrer que si $p \equiv 7 \pmod 8$ alors p divise M_q.

5. Le nombre de Mersenne $M_{23} = 2^{23} - 1 = 8\ 388\ 607$ est-il premier ?

Exercice 3.

1. Calculer le symbole de Jacobi : $\left(\frac{541}{2011}\right)$.

2. Que peut-on en déduire sur l'existence de solutions à la congruence $x^2 \equiv 541 \pmod{2011}$?

3. Montrer que 2011 est premier.

3. En déduire le reste de la division euclidienne de 541^{1005} par 2011.

Exercice 4.

On utilise la correspondance

$$a \longmapsto 0, b \longmapsto 1, c \longmapsto 2, d \longmapsto 3, e \longmapsto 4, f \longmapsto 5, g \longmapsto 6, h \longmapsto 7$$

$$i \longmapsto 8, j \longmapsto 9, k \longmapsto 10, l \longmapsto 11, m \longmapsto 12, n \longmapsto 13, o \longmapsto 14$$

$$p \longmapsto 15, q \longmapsto 16, r \longmapsto 17, s \longmapsto 18, t \longmapsto 19, u \longmapsto 20, v \longmapsto 21$$

$$w \longmapsto 22, x \longmapsto 23, y \longmapsto 24, z \longmapsto 25$$

entre les lettres de l'alphabet et les entiers modulo 26.

On considère le chiffrement affine suivant :

$$\begin{array}{rccc} e: & \mathbb{Z}/26 & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ & x & \longmapsto & 15x + 1 \end{array}$$

1. Expliquer pourquoi ce chiffrement est valide i.e. pourquoi il est bijectif.

2. Quel est le chiffré du texte clair : *hello* ?

3. Quelle est l'application déchiffrement d associée à l'application e ?

4. Déchiffrer le cryptogramme LDL.

* * *